PERANCANGAN DAN IMPLEMENTASI ALGORITMA VEA *(Video Encryption Algorithm)* UNTUK KEAMANAN DATA PADA VIDEO MPEG

SKRIPSI

Diajukan Oleh :

DONY RAHMAWAN **0736010020**

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"

JAWA TIMUR

2011

KATA PENGANTAR

Syukur *Alhamdulillaahi rabbil 'alamin* terucap ke hadirat Allah SWT atas segala limpahan Kekuatan-Nya sehingga dengan segala keterbatasan waktu, tenaga, pikiran dan keberuntungan yang dimiliki penyusun, akhirnya penyusun dapat menyelesaikan Skripsi yang berjudul **"Perancangan dan implementasi algoritma VEA *(Video Encryption Algorithm)* untuk keamanan data pada video MPEG"** tepat pada waktunya.

Skripsi dengan bobot 4 SKS ini disusun guna diajukan sebagai salah satu syarat untuk menyelesaikan program Strata Satu (S1) pada program studi Teknik Informatika, Fakultas Teknologi Industri, UPN "VETERAN" Jawa Timur.

Melalui Skripsi ini penyusun merasa mendapatkan kesempatan emas untuk memperdalam ilmu pengetahuan yang diperoleh selama di bangku perkuliahan, terutama berkenaan tentang penerapan teknologi perangkat lunak *(Software)*. Namun, penyusun menyadari bahwa Skripsi ini masih jauh dari sempurna. Oleh karena itu penyusun sangat mengharapkan saran dan kritik dari para pembaca untuk pengembangan aplikasi lebih lanjut.

Surabaya, 12 Mei 2011

(Penyusun)

UCAPAN TERIMA KASIH

Penyusun menyadari bahwasanya dalam menyelesaikan Skripsi ini telah mendapat banyak bantuan dan dukungan dari berbagai pihak, dan tanpa menghilangkan rasa hormat,, penyusun mengucapan terima kasih kepada:

1. Prof. Dr. Ir. Teguh Soedarto, MP selaku Rektor UPN “Veteran” Jawa Timur.
2. Ir. Sutiyono, MT selaku Dekan Fakultas Teknologi Industri UPN “Veteran” Jawa Timur.
3. Basuki Rahmat,S.Si,MT selaku Kepala Jurusan Teknik Informatika UPN “Veteran” Jawa Timur, dosen wali sekaligus dosen pembimbing I yang telah banyak meluangkan waktu untuk memberikan arahan dan ilmu.
4. Agus Hermanto S.Kom selaku dosen pembimbing II yang telah banyak memberikan bimbingan sampai Tugas Akhir ini terselesaikan.
5. Bapak dan ibu tercinta yang telah memberikan do’a dan dorongan baik moril maupun spiritual. Aries Dwi Irawan S.Kom yang selalu memberikan do’a dan semangat sampai terselesainya Tugas Akhir ini.
6. Teman-teman kuliah khususnya anak-anak Ilmu Komputer angkatan 2007 deddy, faris, borud, fathi, toni, taufik, alan, teman-teman teknik informatika dan system informasi yang tidak bisa saya sebutkan satu persatu. Terima kasih semua atas persahabatan yang begitu indah selama kuliah. N sukses buat kalian semuanya….
7. Teman-teman Formasda *(Forum mahasiswa sidoarjo*) yang telah memberikan semangat dan motivasi sampai Tugas Akhir ini selesai.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

ABSTRAK

Keamanan data multimedia sangat penting dalam akhir-akhir ini. Perkembangan awal *kriptografi* dipusatkan pada data berbentuk tulisan. Algoritma yang digunakan untuk itu mungkin tidak sesuai untuk file multimedia yang mempunyai ukuran yang besar. Untuk itu diperlukannya algoritma lain yang ringan dan aman. Proses enkripsi pada video akan menghasilkan video dengan gambar yang acak. Sebaliknya, proses dekripsi akan mengembalikan video terenkripsi kembali menjadi video asli. *Keyword* yang digunakan pada proses *enkripsi* dan *dekripsi* ini harus sama, jika tidak proses dekripsi tidak akan mengembalikan video yang aslinya.

Algoritma VEA umum digunakan untuk keperluan *enkripsi* video karena kemudahannya dalam implementasi, terutama karena algoritma ini mengenkripsi video bit per bit. Model *enkripsi* dan *dekripsi* pada video MPEG ini dibangun dengan menggunakan bahasa pemrograman Java dan netbeans 6.8.

Dengan adanya permasalahan diatas maka dalam Skripsi ini dibuat sebuah perancangan menggunakan algoritma VEA *(Video Encryption Algorithm)* untuk diimplementasikan pada video MPEG. Dengan memenuhi standart *kriptografi* dan keamanan data.

Kata Kunci : *Algoritma VEA, kriptografi, enkripsi dan dekripsi.*

BAB I

PENDAHULUAN

Dalam bab ini dijelaskan beberapa hal dasar yang meliputi latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, metodologi skripsi serta sistematika penulisan skripsi. Dari uraian tersebut diharapkan, gambaran umum permasalahan dan pemecahan yang diambil dapat dipahami dengan baik.

1.1 Latar Belakang Masalah

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu data, pesan dan informasi. Pengiriman suatu pesan, data dan informasi yang sangat penting membutuhkan tingkat keamanan yang tinggi. Dengan perkembangan teknologi informasi sekarang ini yang begitu pesat, di mana setiap orang akan mudah untuk mendapatkan suatu pesan, data dan informasi. Berbagai cara dilakukan orang untuk mendapatkan data dan informasi tersebut. Mulai dari tingkatan yang mudah sampai kepada cara-cara yang lebih rumit. Dan berbagai cara pula orang berusaha untuk melindungi pesan tersebut agar tidak dapat diketahui oleh orang yang tidak memiliki hak atas pesan atau data tersebut.

Ilmu yang mempelajari tentang proses pengaman data adalah kriptografi. Secara umum ada dua jenis kriptografi, yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik adalah suatu algoritma yang menggunakan satu kunci untuk mengamankan data. Dua teknik dasar yang biasa digunakan adalah substitusi dan transposisi (permutasi). Sedangkan kriptografi modern adalah algoritma yang lebih kompleks daripada algoritma kriptografi klasik, hal ini disebabkan algoritma ini menggunakan komputer. Algoritma yang akan penulis gunakan adalah algoritma kriptografi modern.

Pada model enkripsi ini dipilih algoritma VEA *(Video Encryption Algorithm)* untuk diimplementasikan pada enkripsi file multimedia. Algoritma VEA tersebut digunakan karena dinilai ringan dan cocok untuk diterapkan pada video yang pada umunya berukuran besar. Untuk meningkatkan keamanan proses enkripsi, algoritma VEA yang ada dimodifikasi dengan menambahkan algoritma kriptografi DES. Hal ini mengakibatkan operasi yang dilakukan bukan lagi per bit, melainkan per blok-blok slice dari gambar video

Dua hal yang dapat diperhatikan dari enkripsi data multimedia adalah: pertama, ukuran data multimedia biasanya sangat besar. Sebagai contoh, ukuran data dari video MPEG-1 berdurasi dua jam kira-kira 1 GB. Kedua, data multimedia harus diproses real-time. Memproses sejumlah besar data saat real-time dengan algoritma kriptografi yang

rumit akan memperberat kinerja komputer serta jaringannya, dan juga tidak nyaman bagi orang yang menonton video tersebut secara real-time karena hal tersebut dapat berpengaruh juga pada delay video yang sedang ditontonnya. Untuk beberapa jenis aplikasi video komersil, seperti program *pay-per-view*, informasi yang terdapat sangat banyak, tetapi nilai dari informasi tersebut sangat rendah.

1.2 Rumusan masalah.

Berangkat dari latar belakang tersebut diatas maka dirumuskan permasalahan dalam tugas akhir ini adalah sebagai berikut :

1. Bagaimana membuat system applikasi yang dapat melakukan enkripsi dan dekripsi data pada video berformat MPEG ?
2. Bagaimana mengamankan dan merahasiakan berkas-berkas digital yang dianggap tidak layak untuk diketahui public.
3. Bagaimana cara mengembalikan video yang sudah dienkripsi menjadi video asli. Sehingga hasilnya bisa dilihat secara utuh oleh user yang memiliki hak akses dan mengetahui kuncinya.

1.3 Batasan masalah

Agar tidak terjadi kesalahan persepsi dan tidak meluasnya pokok bahasan, maka terdapat batasan-batasan masalah sebagai berikut:

1. Applikasi ini dibuat dengan menggunakan bahasa pemrograman java netbeans 6.8
2. Sistem hanya melakukan enkripsi dan dekripsi pada file video MPEG.
3. Dilakukannya proses dekripsi guna mengetahui video aslinya.
4. System akan menghasilkan file baru pada saat proses enkripsi dan dekripsi
5. Kunci dalam proses enkripsi dan dekripsi bisa berupa angka, huruf, serta kombinasi angka dan huruf.

1.4 Tujuan

Mengacu pada perumusuhan masalah diatas, tujuan yang hendak dicapai dalam penyusunan tugas akhir ini adalah :

1. Menerapkan teknologi enkripsi pada berkas digital dengan metode VEA *(Video Encryption Algorithm)* untuk keamanan data pada video berformat MPEG.
2. Mengamankan video atau berkas digital yang didalamnya mengandung unsur pornografi, sara, teroris, dan kekerasan. sehingga tidak sampai meluas ke masyarakat.
3. Melindungi hak cipta dan karya-karya digital dari pembajakan dan pencurian oleh pihak yang tidak bertanggung jawab.
4. Merahasiakan video-video yang dianggap penting, seperti : video dokumenter Negara, video perjuangan, dan video sejarah. Dengan adanya kunci yang hanya diketahui oleh user maka video tersebut dapat terjaga kerahasiaanya.

1.5 Manfaat

Manfaat yang diperoleh dalam pembuatan aplikasi ini antara lain :

1. Dihasilkan suatu aplikasi yang dapat melakukan proses enkripsi dan dekripsi dengan menggunakan metode VEA.
2. Dapat mengamankan data atau file video yang didalamnya terdapat unsur pornografi, sara dan kekerasan. Sehingga tidak sampai menyebar luas kemasyarakat.

1.6 Metodologi Pembuatan Tugas Akhir

Pembuatan Tugas Akhir ini terbagi menjadi beberapa tahapan sebagai berikut :

1.Studi Literatur

Pada tahap ini dilakukan pengumpulan dokumen-dokumen referensi tentang *Kriptografi*, keamanan data, algoritma VEA, proses *enkripsi* dan *dekripsi*, struktur komponen video.

2.Pembuatan program

Pada tahap ini dilakukan *coding* untuk membuat sebuah program sederhana untuk dapat melakukan proses enkripsi dan dekripsi pada MPEG. Sehingga menghasilkan *output* yang dapat dianalisa.

3.Analisa hasil

Program yang telah selesai akan dilakukan uji coba dan kemudian dilakukan analisa terhadap hasil dari program tersebut.

4.Penyusunan Buku Tugas Akhir

Pada tahap terakhir ini disusun buku sebagai dokumentasi dari pelaksanaan Tugas Akhir. Dokumentasi ini dibuat untuk memudahkan orang lain yang ingin mengembangkan teknologi enkripsi dengan menerapakan metode algoritma *VEA (Video Encryption Algorithm).*

1.7 Sistematika Penulisan

Dalam laporan tugas akhir ini, pembahasan disajikan dalam enam bab dengan sistematika pembahasan sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini dikemukakan hal-hal yang menjadi latar belakang masalah, perumusan masalah, pembatasan masalah, tujuan serta keterangan mengenai sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini dibahas teori yang mendukung pokok pembahasan tugas akhir antara lain teori tentang *netbeans 6.8, kriptografi,* keamanan data dan algoritma VEA,

BAB III ANALISA & PERANCANGAN SISTEM

Pada bab ini akan dibahas mengenai identifikasi masalah, analisis dan pemecahan masalah mengenai algoritma yang digunakan pada proses enkripsi dan proses dekripsi file multimedia.

BAB IV IMPLEMENTASI SISTEM

Pada bab ini menjelaskan tentang implementasi system, berisi langkah-langkah implementasi perancangan system dan hasil implementasi system dengan tujuan yang telah diharapkan.

BAB V : UJI COBA

Pada bab ini akan dijelaskan mengenai analisa *output* baik dari proses enkripsi atau proses dekripsi menggunakan metode VEA *(Video Encryption Algorithm).*

BAB VI PENUTUP

Pada bab ini dibahas mengenai kesimpulan dari perancangan dan pembuatan tugas akhir ini terkait dengan tujuan dan permasalahan yang ada, serta saran untuk pengembangan system dimasa mendatang.